Director of Central Intelligence Directive

Type: 3 **Number:** 29
Subject: CONTROLLED ACCESS PROGRAM OVERSIGHT COMMITTEE
Category: 3-DCI Advisory Bodies

DIRECTOR OF CENTRAL INTELLIGENCE DIRECTIVE 3/29

Controlled Access Program Oversight Committee

(Effective 2 June 1995)

Pursuant to the provisions of the National Security Act of 1947, as amended, and Executive Orders 12333 and 12958, the Controlled Access Program Oversight Committee is hereby established to assist the Director of Central Intelligence in carrying out his responsibilities for controlled access programs within the National Foreign Intelligence Program.

APPROVED FOR RELEASE
12-99

1. Controlled Access Programs

The following controlled access programs are covered by this Directive:

1.1 Sensitive Compartmented Information (SCI). The National Security Act of 1947 and Executive Orders 12333 and 12958 grant the Director of Central Intelligence (DCI) the authority to protect classified information concerning or derived from intelligence sources, methods, or analytical processes. This Directive covers all programs within the SCI control system.

1.2 Special Access Programs Pertaining to Intelligence Activities. The National Security Act of 1947 and Executive Order 12958 authorize the DCI to create special access programs pertaining to intelligence activities (including special activities, but excluding military operational, strategic and tactical programs). This Directive covers all such programs.

1.3 Restricted Collateral Information. This Directive also covers programs other than SCI or special access programs that impose controls governing access to classified intelligence information or control procedures beyond those normally provided for access to Confidential, Secret, or Top Secret information, and for which funding is specifically identified. This Directive does not cover access [redacted]

2. Controlled Access Policy

2.1 All proposals to create or maintain controlled access programs shall be reviewed by the Controlled Access Program Oversight Committee (CAPOC). Controlled access programs shall be kept to an absolute minimum and only established and maintained to protect the Nation's most sensitive and critical intelligence information. Decisions to establish controlled access programs shall be based on a risk assessment, considering the sensitivity, risk of disclosure and exploitation, and value of the information to be protected.

2.2 The DCI or DDCI shall determine whether to create, modify, or terminate controlled access programs. Creation or continuation of controlled access programs shall only be made upon a specific finding that:

a. the vulnerability of, or threat to, specific information is exceptional; and
b. the normal criteria for determining eligibility for access applicable to information classified at the same level are not deemed sufficient to protect the information from unauthorized disclosure; or
c. the program is required by statute.

2.3 Controlled access programs shall be reviewed annually. Any such program not granted approval to continue shall be decompartmented or terminated.

2.4 Only the DCI or DDCI may create, modify, or terminate controlled access programs.

3. CAPOC

3.1 The CAPOC provides a mechanism for supporting the DCI in the effective execution of DCI responsibilities for the controlled access programs and activities within the National Foreign Intelligence Program (NFIP). These responsibilities include ensuring the creation and continuation of only those controlled access programs necessary to protect sensitive intelligence information; monitoring the implementation of controlled access programs; directing program and performance audits and evaluations as necessary; and ensuring there is no conflict or unnecessary duplication between controlled access programs within the NFIP and other government programs by working with the appropriate representatives from those programs.

3.2 The CAPOC shall review and validate controlled access programs. The DCI or DDCI may waive review by the CAPOC for programs covered by equivalent oversight mechanisms, or when review by the CAPOC is unnecessary to carry out the DCI's responsibilities.

3.3 The CAPOC shall review the creation of new controlled access programs and validate existing controlled access programs. The review shall include:

a. the justification for controlled access designation or continued designation;
b. whether the controlled access program duplicates any other program;
c. whether any other program would benefit from the information protected by the controlled access program or activity;
d. verification of compliance with US laws, regulations, and pertinent policies and procedures, [redacted]

e. whether the unacknowledged or cover status of the program should be continued, if applicable;
f. authorizations to require security standards in excess of standards contained in DCIDs or other applicable documents; and
g. such other matters as agreed to by the DCI and heads of agencies involved.

3.4 The membership of the CAPOC shall include:

a. the DCI or the DDCI;
b. the DepSecDef if the controlled access program is managed by a Defense agency;
c. the head or deputy head of the agency(s) responsible for the controlled access program being reviewed (for the CIA, the Executive Director for the Central Intelligence Agency shall attend as the agency head); and
d. the Executive Director for Intelligence Community Affairs.

3.5 The DCI may invite other individuals to participate in particular CAPOC reviews.

3.6 The DCI shall call meetings of the CAPOC. Minutes of the meetings shall be taken, including the decisions of the DCI or DDCI, and the findings required by 2.2, above.

3.7 The DCI or DDCI may alter the procedures of the CAPOC when reviewing a controlled access program of special sensitivity.

3.8 As necessary, the CAPOC will approve policies, procedures, and security standards pertaining to controlled access programs, consistent with the politics of the Security Policy Board, pertaining to controlled access programs.

4. Controlled Access Program Coordination Office (CAPCO)

4.1 The Controlled Access Program Coordination Office (CAPCO) is established within the Office of the DCI. The Director of the CAPCO shall be appointed by the DCI.

4.2 The CAPCO shall conduct the following activities:

a. develop risk assessment criteria and procedures for the review and evaluation of controlled access programs;
b. provide guidance to Intelligence Community agencies concerning submissions to the CAPOC;
c. coordinate with other controlled access program oversight fora to meet the review requirements of the CAPOC;
d. coordinate the CAPOC agenda and monitor directed taskings;
e. review and evaluate agency submissions and make recommendations to the CAPOC;
f. provide secretariat services for the CAPOC; and
g. maintain a register of all controlled access programs in the NFIP.

4.3 The CAPCO shall work in concert with the agency whose controlled access program is being reviewed in preparing material for the CAPOC.

4.4 The CAPCO shall coordinate security policies with the Security Policy Board and the Special

5. Responsibilities of Intelligence Community Agencies

Heads of Intelligence Community agencies with controlled access programs covered by this Directive shall

a. recommend the creation, modification, or termination of controlled access programs, pursuant to the standards in Section 2 above;
b. conduct an annual review of each program, including compartments and subcompartments thereof, and document the review. At a minimum, the review shall include the items mentioned in Section 3.3 above;
c. for each controlled access program, ensure the appointment of a security manager who is responsible for administration of security for the program, including record maintenance;
d. ensure for any controlled access program involving industry, that proper officials within the contractor's facility, to include the facility security office and other appropriate corporate officials, are cognizant of the nature and extent of their facility's involvement in the program;
e. ensure proper reporting of: 1) adverse information on personnel with access to a program to the cognizant security office; and 2) instances of suspected waste, fraud, and abuse to the Inspector General of the agency;
f. designate an official point of contact to the CAPOC; and
g. for agencies with more than one controlled access program, designate a central office to coordinate the activities in this section. The central office shall be the official point of contact to the CAPOC.